USDA / DA / OPPM / PDSD
www.usda.gov/da/pdsd

PERSONNEL & DOCUMENT SECURITY DIVISION

PDSD NEWS

PLANTING THE SEEDS TO ACHIEVE PERSONNEL SECURITY AND INFORMATION SECURITY GOALS.

New & Improved PDSD Website

The Personnel & Document Security Division has redesigned the look and feel of our website to meet the eGov Web Presence initiative.
Check us out at http://www.usda.gov/da/pdsd/.

Our new site offers our customers better access to the services and guidance we provide. On our home page, you will find links to the latest news and spolights on personnel and information security issues. The most convenient addition is the "I Want To" section on the right column. Here you will find links to common needs our customers have such as accessing e-QIP or submitting a request to have a clearance passed. On the left column, you will find our five main subject areas: Personnel Security, Information Security, Industrial Security, Online Forms, and Resources.

The Personnel Security Branch (PSB) home page includes an overview of the background investigation process, common questions & answers on investigations, access to e-QIP, and a link to the Automated Security Briefing System (soon to be announced) .

The Information Security Staff (ISS) home page includes information on Sensitive Compartmented Information Facilities (SCIF), access to the USDA Classified Information Desktop Reference, and common questions & answers relating to information security matters.
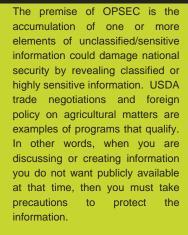
The Online Forms section allows our customers to access commonly used personnel and information security forms such as the Request to Pass a Security Clearance (AD-1189). Additional forms will become available as they complete the approval process with OCIO.

The Resources section is essentially a personnel and information security reference library that includes PDSD bulletins, directives, and policies.

Check back regularly for updated information to include any staff and agency points-of-contact changes. If you would like to see any additions that will help you work better with us, please email us at pdsd@usda.gov.

OPERATIONS SECURITY (OPSEC) AND USDA

Operations Security (OPSEC) is formally defined as an analytic process used to deny adversaries information – generally unclassified – concerning our intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning processes or operations. Clearly, a Department of Defense initiated program, yet it does have application at USDA.

The premise of OPSEC is the accumulation of one or more elements of unclassified/sensitive information could damage national security by revealing classified or highly sensitive information. USDA trade negotiations and foreign policy on agricultural matters are examples of programs that qualify. In other words, when you are discussing or creating information you do not want publicly available at that time, then you must take precautions to protect the information.

Some precautions that are simple, free, and very effective are identified in the next column. If you have questions or concerns about OPSEC, you can call the Information Security Staff, Personnel and Document Division, OPPM at (202) 720-7373.

1. Turning a cell phone off does not guarantee that it is not transmitting information so it is best to remove your cell phone battery before meetings that will include discussions of classified or security sensitive information.
2. Disconnect conference-calling equipment when it is not needed. They have the capability of transmitting conversations when not turned on.
3. Do not talk sensitive information on a cell phone that is not encrypted for classified conversations. Assume all calls are being eavesdropped.
4. If you have an encrypted cell phone and plan on talking sensitive or classified information, be aware of the people around you. If they can hear your conversation, they must have the appropriate clearance and a need-to-know the information.
5. Telephones located in offices and conference rooms should have ISDN identified on the phone. If it does not, then it can act as a transmitter of information.
6. Rethink what you are throwing away in the recycle and trashcans. Assume an adversary is collecting information from USDA trash. If in doubt, shred documents.
7. Before sending an email ask yourself, "If this was published in the Washington Post would it reveal sensitive information or embarrass myself or USDA? Can this email along with others I have sent out, create sensitive or classified information?" If so, you may want to reword your email.
8. Be wary of conference and symposium attendees or uninvited emails asking for specific program information. If you do not know the individual and their need for the information, you can share information that is already publicly available, or refer them to the USDA Public Affairs Office.

ESSENTIAL POINTERS TO A SOLID
e-QIP Submission

As we near the end of our second year using the Office of Personnel Management's Electronic Questionnaires for Investigations Processing (e-QIP) system to process applicants for national security and public trust investigations, agencies should have some established processes for e-QIP initiation.

As an example, all USDA agencies should be notifying applicants and instructing them on how to access the e-QIP system with an e-mail containing the e-QIP brochure attached. Please do not simply send an e-mail with just the e-QIP Gateway located at www.opm.gov/e-qip without providing any instructions. The e-QIP Gateway allows the applicant to view or print the official e-QIP Brochure, access a list of frequently asked questions, and access e-QIP to begin filling out their security questionnaire, which is why it is so important to give the applicant instructions before getting started. For an example of an email notification letter, please contact Vet Thorpe at Arviet.thorpe@usda.gov.

Here are some helpful tips and reminders to our agency points-of-contact (POCs) regarding e-QIP submissions:

- Put the e-QIP case number on the fingerprint chart submissions if you are submitting them to OPM electronically.
- Under the Agency Use Block, the SON and SOI are always AGOO if the request is going through PDSD.
- Under the Agency Use Block, block M should always have NPI checked.
- Please check to ensure the OPAC block has the correct number of digits (leaving one out will get a form kicked back from OPM).
- Make sure all pages are scanned in correctly.
- Make sure the Agency Use Block in e-QIP matches what is requested on the Request for Services form.

See page 5 for common user Q&A.

BULLETIN WATCH: #06-05

On March 7th, PDSD issued bulletin #06-05, Background Investigation Processing Requirements.

In an effort to meet the timeliness expectations set forth by the Office of Management and Budget (OMB) as a result of the Intelligence Reform and Terrorism Protection Act, PDSD is now requiring agencies to submit completed security packages within 7 calendar days from the date the Subject signed the form and required releases.

The entire bulletin can be read at http://www.usda.gov/da/pdsd/bulletin06-05.pdf.

ADVICE AND PLANNING: REINVESTIGATIONS

The Investigative Standards for Background Investigations for Access to Classified Information, established as a result of Executive Order 12968, requires individuals with Top Secret (TS), Sensitive Compartmented Information (SCI), or "Q" access to undergo a periodic reinvestigation at any time following the completion of, but no later than, five years from the date of the previous investigation.

Based upon recommendations from the personnel security community, the President approved amendments to alter the scope of periodic reinvestigations by eliminating the absolute requirement for coverage of references and neighborhoods in cases when no information of security concern is admitted or developed.

In response to this change, OPM has developed a new product, the Phased Periodic Reinvestigation (PPR), effective October 1, 2005. Agencies now have two products to choose from when reinvestigating individuals for TS, SCI, or Q access, the SSBI-PR or the PPR. Agencies are reminded that Executive Order 12968 requires background investigations be reciprocally accepted by all agencies. This applies regardless of whether the reinvestigation was an SSBI-PR or a PPR.
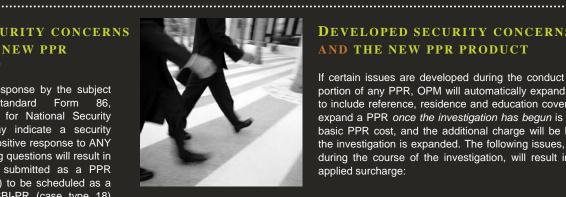
Option One: Full Scope Single-Scope Background Investigation, Periodic Reinvestigation (SSBI-PR). OPM will continue to offer the full scope SSBI-PR with full coverage and issue resolution for agencies that choose to use this product. All SSBI-PR investigations will now include issue resolution.

Option Two: Phased Periodic Reinvestigation (PPR). The PPR can be requested if the subject does not disclose anything of a security concern as part of the background information furnished for investigation. The section below indicates the questions on the SF86 that OPM will review to determine whether a PPR may be requested. OPM will automatically convert any PPR request to the full scope SSBI-PR product, at case scheduling, if there are any positive responses to one or more of the security concern questions on the SF86. The agency will be billed at the SSBI-PR rate. Any investigation originally scheduled as a basic PPR that develops information of a security concern during the course of the investigation will be expanded to meet the full SSBI-PR requirements. A surcharge will be applied to all expanded cases.

The case type for the SSBI-PR remains 18 and the price starts at $2050. The case type for the PPR is 19 and the price starts at $1625.

SF86 SECURITY CONCERNS AND THE NEW PPR PRODUCT

A positive response by the subject on the Standard Form 86, Questionnaire for National Security Positions, may indicate a security concern. A positive response to ANY of the following questions will result in investigations submitted as a PPR (case type 19) to be scheduled as a full scope SSBI-PR (case type 18) and billed accordingly.

A positive response by the subject on the Standard Form 86, Questionnaire for National Security Positions, may indicate a security concern. A positive response to ANY of the following questions will result in investigations submitted as a PPR (case type 19) to be scheduled as a full scope SSBI-PR (case type 18) and billed accordingly.

SF 86 Question	Response
8a CITIZENSHIP	"I am not a U.S. Citizen" checked
8d DUAL CITIZENSHIP	Checked
17 YOUR FOREIGN ACTIVITIES	A positive response to questions b, c, or d.
21 YOUR MEDICAL RECORD	A positive response
23 YOUR POLICE RECORD	A positive response to questions a, b, c, d, e, or f
24 YOUR USE OF ILLEGAL DRUGS	A positive response to questions a, b, or c
25 YOUR USE OF ALCOHOL	A positive response
26 YOUR INVESTIGATIONS RECORD	A positive response to question b
30 YOUR ASSOCIATION RECORD	A positive response to questions a or b

View FIN 05-04 at http://www.opm.gov/extra/investigate/fin-2005/fin05-04.asp.

If you have any questions concerning the type of reinvestigation product you should use, please contact the Personnel Security Branch at 202/720-7373 (PDSD).

DEVELOPED SECURITY CONCERNS AND THE NEW PPR PRODUCT

If certain issues are developed during the conduct of the field-work portion of any PPR, OPM will automatically expand the investigation to include reference, residence and education coverage. The cost to expand a PPR *once the investigation has begun* is in addition to the basic PPR cost, and the additional charge will be billed at the time the investigation is expanded. The following issues, when developed during the course of the investigation, will result in expansion and applied surcharge:

- Evidence that the Subject is not a U.S. citizen, or has renounced or otherwise lost his U.S. citizenship since the time of the last investigation;

- Evidence that the Subject is a dual citizen or has obtained dual citizenship since the time of the last investigation;

- Evidence that the Subject has been employed by or acted as a consultant for any foreign government, firm or agency; that the Subject has engaged in any contact with a foreign government or its establishments or representatives on other than official U.S. government business; that the Subject holds or has been issued a foreign passport;

- Evidence that the Subject has undergone mental health treatment (except marital, family or grief counseling, not related to violence by the Subject) since the last investigation, whether this treatment began before or after the last investigation;

- Evidence that the Subject has been charged with or convicted of any criminal offenses (excluding traffic violations resulting in fines less than $150) since the last investigation;

- Evidence that the Subject used any drugs since the last investigation;

- Evidence that the Subject has abused alcohol or has received any alcohol-related treatment or counseling since the last investigation;

- Evidence that the Subject has had a clearance or access authorization denied, suspended or revoked, or has been debarred from Federal employment since the last investigation; and

- Evidence that the Subject has associated with any individuals or groups dedicated to the violent overthrow of the United States government or that the Subject has acted to do so.

IMPROVING THROUGH TEAMWORK

WHAT IS NEED-TO-KNOW (NTK)?

NTK is the determination by an authorized holder of classified or sensitive information that access to the information is required by another appropriately cleared individual to perform his or her official duties.

Everyone has the individual responsibility to ensure NTK before sharing information with another individual. If you are sharing classified information, you must verify the individual has the appropriate security clearance, as well as, NTK.

This is especially important during meetings. If you are leading a meeting, it's your responsible to control the conversation and ask people to talk about something after the meeting if all the attendees don't have a NTK.

E-QIP UPDATES

SF 85 implementation: The PDSD is currently developing plans to implement the final phase of e-QIP, which entails setting up USDA Human Resources offices to use the Standard Form 85 (SF 85), "Questionnaire for Non-sensitive Positions" to process National Agency Checks with Inquiries (NACI) directly to the Office of Personnel Management (OPM). The PDSD has met with the OPM to discuss initially rolling out the SF 85 to select agencies whose HR structure is more centralized, then gradually including agencies with a more decentralized HR structure. In addition, the decentralized agencies have been asked to make an effort to consolidate NACI processing to ease PDSD's management of e-QIP system accounts and more easily train new users. The PDSD has selected the National Finance Center as the first test agency for the SF 85 with an expected implementation date of June 2006.

E-QIP Version 2.0: The OPM will begin testing the 2.0 version of e-QIP in April 2006. USDA's PDSD has been asked to assist in testing the newer version on the OPM training site, which is tentatively scheduled for availability on June 1, 2006. The newer version allows for easier movement between screens, maneuvering through the system without logging out, and viewing split screens. The PDSD plans to set up regular training sessions for existing users, beginning in May, and will offer multiple training sessions for new users, beginning in June. Sessions will be held in the sub-basement of the South Building. As May approaches, we will post a training schedule on our website, located at http://www.usda.gov/da/pdsd/ .

If you have any questions concerning NTK, please contact PDSD at 202/720-7373 (PDSD). You may contact your agency point-of-contact to request clearance verification on an individual when in doubt before sharing classified information. For a listing of the agency points-of-contact, please visit our website at **http://www.usda.gov/da/pdsd/**.

NEW! THE USDA INFORMATION SECURITY DRAFT REGULATION AND MANUAL ARE NOW ONLINE FOR YOUR REVIEW AND COMMENT. THIS INTERIM GUIDANCE CAN BE FOUND ON THE PDSD WEBSITE AT http://www.usda.gov/da/pdsd/.

PARTICIPATING WITH PERSEREC:
MEASURING THE QUALITY OF PERSONNEL SECURITY INVESTIGATIONS

The quality and efficiency of personnel security clearance programs across the federal government have recently received a great deal of attention following the terrorist attacks of September 11, 2001, the increase in positions requiring security clearances, and the release of the Intelligence Authorization Act of 2004. To help address concerns surrounding the quality of personnel security investigations (PSI), the Defense Personnel Security Research Center (PERSEREC) has developed a set of rating scales called the Background Investigation Quality Rating Form (BI-QRF) that can be used to get feedback from adjudiators about their level of satisfaction with the quality of investigations. PERSEREC hopes to identify problematic aspects of investigative reports for adjudication, document investigation strenghts and weaknesses, address reciprocity concerns, supplement traning efforts, and monitor PSI service contracts.

The Personnel Security Branch (PSB) is in the process of joining this study and we look forward to finding ways to improve the adjudication process.

FREQUENTLY ASKED E-QIP QUESTIONS

1.   What is the process for completing my SF-86 using e-QIP?
Once you have been notified that you have access, login by entering your security number and answering the three Golden questions. After logging in the first time, you will be prompted to change your golden questions to ensure the security of your data. After changing your Golden questions, e-QIP presents you with the Main Menu. Select the link entitle, "Enter Your Data" from the main menu screen. After reading all instructions, you can now begin entering your personal data. In order to ensure the completeness of your data, a validation routine will run after each page is submitted. The validation routine will point out any errors and provided detailed instructions on how to satisfy each incorrect or missing item. When you are satisfied that your form is complete, select the "Display Your Data" link from the main menu. After a final review of your date, select the "Certify/Submit" button to finish your form. On the last screen make sure to print a copy for your records and print and sign each form that has a blank for your signature. Only after you have printed and signed the appropriate signature pages, should you click on the final link entitled, "Release Request/Transmit to Agency."

2.   I cannot login to e-QIP. What should I do?
After verifying all system requirements listed in the e-QIP brochure, contact your sponsoring agency to verify that you currently have an active request in the e-QIP system.

3.   When I try to login, e-QIP displays golden questions that I have never created, or that I don't know the answer to. What should I do?
If you are getting "bogus" Golden Questions that you do not recognize or do not know the answer to, please contact your sponsoring agency to verify that you currently have an active request in the system or to request that your Golden questions be re-set to the default values.

4.   I have just logged in. I don't know where to start from the Main Menu. What do I do?
Click on the link entitled "Enter Your Data" to begin entering your personal data.

5.   What does the "Submit" button do?
The "Submit" button saves any data that you have entered on the current screen.

New Guidance for Contracting Classified Work

The Department of Defense has oversight of USDA Contractors performing classified work.   There is a new National Industrial Security Program Manual (NISPOM) which provides contractor and government responsibilities. You can find the NISPOM at:

http://www.dtic.mil/whs/directives/corres/html/522022m.htm

USDA has an Industrial Security Program and can offer guidance and assistance. Please call Diane Dixon, Chief, Information Security Staff, PDSD at (202) 720-7373 for assistance.

EMAIL US AT PDSD@USDA.GOV
CONTACT US AT 202/720-7373
THIS NEWSLETTER IS FOR USDA PURPOSES.

Federal Register Notice Required Before Identity Proofing Nonemployee Associates under HSPD-12

The USDA Office of General Counsel (OGC) recently advised that a Federal Register notice must be issued before identity proofing nonemployee affiliates. Examples of nonemployee affiliates are cooperative agreement and state and local employees. OGC also recommended that USDA change the name "nonemployee affiliates" to simply "employees" for the purpose of Federal Information Processing Standards 201 and HSPD-12 implementation.

Agencies should continue planning which of these employees (formally called nonemployee affiliates) should be identity proofed and when, but not begin the actual identity proofing until notified to do so. HSPD-12 implementation teams will be receiving complete information on this change in the near future.